BY ORDER OF THE COMMANDER
TWENTY-FIFTH AIR FORCE (ACC)

25 AIR FORCE INSTRUCTION 31-101

7 FEBRUARY 2017

Security

SECURITY PROCEDURES FOR HEADQUARTERS TWENTY-FIFTH AIR FORCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 25 AF/A2S

Certified by: 25 AF/A2/3
(Col Timothy Sipowicz)
Pages: 34

This publication implements Air Force Policy Directive (AFPD) 31-1, *Integrated Defense,* and AFPD 16-14, *Security Enterprise Governance.* It implements broader guidance found in DoDM 5105.21-V1-3, *Sensitive Compartmented Information Administrative Security Manual,* and Air Force Instruction (AFI) 31-101, *Integrated Defense.*

This publication directly applies to all military and civilian personnel assigned to the Headquarters (HQ) Twenty-Fifth Air Force (25 AF) and its subordinate organizations located on Joint Base San Antonio (JBSA)-Lackland. In addition, this instruction is applicable to our mission partners located within 25 AF facilities located on JBSA-Lackland. This instruction does not apply to 25 AF-aligned Air National Guard and Air Force Reserve units and personnel. The use of the prescribed 25 AF forms is voluntary for 25 AF subordinate organizations; however, the use of the forms constitutes compliance with the guidance herein.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct supplements must be routed through the OPR prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (e.g., T-0, T-3) number following the compliance statement. Requests for waivers must be submitted through chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Maintain records created as a result of the processes prescribed in this

publication in accordance with (IAW) AFMAN 33-363, *Management of Records*, and disposed of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. Contact your supporting Records Manager as required. This publication does not generate information collection and reports as outlined in AFI 33-324, *The Air Force Information Collections and Reports Management Program*.

Chapter 1

PRIMARY PROGRAM RESPONSIBILITIES

1.1. 25 AF Security Office (A2S) :

1.1.1. Acts as the Headquarters (HQ) 25 AF, Special Security Officer (SSO).

1.1.2. Manages the Sensitive Compartmented Information (SCI) security program and oversees SCI security functions.

1.1.3. Provides prepublication review frequently in coordination through Public Affairs.

1.1.4. Maintains appropriate accreditation documentation for each Sensitive Compartmented Information Facility (SCIF) under the organization's security cognizance.

1.1.5. Provides support to special access programs (SAPs) based on approved co-utilization agreements.

1.1.6. Provides physical security program management of the HQ 25 AF complex which encompasses buildings 2000, 2007, 2012 and 2019. Buildings 2000 and 2007 are also designated as a Restricted Area, IAW AFI 31-101, *Integrated Defense*. The Restricted Area boundary is further marked with AFVA 31-101, *Restricted Area Warning Sign,* on each entry door.

Chapter 2

ENTRY CONTROL (BUILDING 2000/2007 EXTERIOR DOORS)

2.1. Entry Credentials (EC) . ECs are used to gain entry to the complex as well as aid internal circulation control within the restricted area and 25 AF buildings. ECs are United States Government property and must be safeguarded at all times. Authorized ECs include: 25 AF Forms 101, 101T, 101DV, 101C, 101CT, 101R, 101F, 101FT, 102, 102T, 102DV, 102C, 102CT, 102R, 102FT, 103, 103DV and 103E. 25 AF Visual Aid 31-103, *Entry Credential Background*, is utilized as an anti-counterfeiting background for 25 AF EC photographs. Individuals with SCI access should immediately report to 25 AF/A2S any instances of individuals found in the SCIF or attempting to enter the SCIF utilizing an unauthorized entry credential or no credential at all.

2.1.1. EC Wear Requirements. ECs will be worn conspicuously below the neck, above the waist, and between the shoulders on the front of the outer-most garment with the front (photograph, "T", "DV" or "Escort Required") facing outward at all times while inside the SCIF. Upon exit, remove (do not display) and secure the EC. **Note:** Only ECs containing badge holder's photographs may be taken outside the HQ 25th Air Force cantonment fenced in area; all other badges—to include temporary, visitor, and DV—must remain inside the cantonment fenced in area.

2.2. Unescorted Entry into the SCIF. Locally assigned personnel with Top Secret clearances and SCI access, entry authority, and 25 AF Forms 101, 101C, 101R, and 101F are authorized unescorted SCIF entry. Likewise, visitors with Top Secret clearances and SCI access, entry authority, and 25 AF Forms 101T, 101DV, 101CT and 101FT are authorized unescorted SCIF entry. **Note:** Entrance to interior rooms requires owner/user concurrence.

2.2.1. Unescorted SCIF entry procedures. Access to the SCIF is controlled through use of proximity access control card readers. Individuals must have a proximity access control badge with access privileges granted. Personal Identification Numbers (PIN) will be required with the proximity badges. Light Emitting Diodes (LED) on the access control reader will alternate blinking red/green continuously indicating the reader is communicating with the annunciator. **Note:** Unit Security Managers provide training to assigned personnel prior to EC issue, document the training via local form (see **Attachment 2**), and maintain the documentation for program review.

2.2.1.1. Place proximity badge in opposite hand from the one you'll use to input your PIN. This prevents multiple readings.

2.2.1.2. Hold (do not wave) your badge directly in front of the reader until you hear two audible beeps.

2.2.1.3. Within 5 seconds, input your 4-digit PIN followed by the pound (#) sign. **Note:** If not completed in 5 seconds, pause for a brief moment to allow the system to reset, then redo the entire process beginning with **paragraph 2.2.1.1**. EXCEPTION: Authorized personnel opening exterior SCIF doors may allow other authorized personnel to enter the SCIF behind them, after validating their entry credentials and photo. Visual recognition is not a sufficient validation – all personnel entering the SCIF must display their EC.

2.2.2. Unescorted SCIF Exit Procedures. When exiting the SCIF, press the panic hardware (door release bar) and push door outward. Exit the SCIF and ensure the door closes securely before walking away. EXCEPTION: Authorized personnel departing the SCIF may allow other authorized personnel to exit the SCIF behind them, after validating their entry credentials and photo. Visual recognition is not a sufficient validation – all personnel exiting the SCIF must display their EC. If an authorized individual is waiting to enter as you exit the door, ensure they have the proper unescorted entry credential before allowing them entry to the SCIF.

2.3. Escorted Entry into the SCIF. Personnel without SCI access will be escorted for the duration of their visit in the SCIF. Visitor Control or the satellite account holder will issue them the appropriate version of the 25 AF Form 102 or 103 based on their security clearance and personnel status (i.e., civilian, contractor, etc.). If the temporary EC is issued by Visitor Control utilizing the 25 AF Form 104, there is no requirement to enter the visitor's information on the AF IMT 1109, *Visitor Register Log*, located at the four SCIF entry points listed in **para 2.3.1** below.

2.3.1. Escort Procedures within the SCIF. Personnel possessing a 25 AF Form 102 requiring entry to the SCIF must report to one of four areas to wait for their escort: Building 2000 first floor foyer, building 2000 courtyard side foyer, building 2007 courtyard side foyer, and building 2007 parking lot side. All other personnel requiring escorted entry into the SCIF must report to an Entry Control Point (ECP) or Visitor Control to wait for their escort.

2.3.2. Escorted entry applies to individuals with official business to perform within the SCIF and who have not been granted unescorted entry. Uncleared dependent family members are permitted to be escorted into the SCIF for official functions like promotion ceremonies, retirements, open houses and other officially sanctioned events. Visitors for non-official functions will be denied entry to the SCIF.

2.3.2.1. Escorts will:

2.3.2.1.1. Be trained and certified annually.

2.3.2.1.2. Meet and positively identify individuals requiring escorted entry outside the SCIF boundary.

2.3.2.1.3. Only print visitor and escort official point of contact information on the AF IMT 1109 visitor sign-in log located at building 2000 first floor foyer, building 2000 courtyard side foyer, building 2007 courtyard side foyer, and building 2007 parking lot side when the visitor either possesses a 25 AF Form 102/103 series picture badge or has been issued a 25 AF Form 102/103 series temporary badge from a satellite account.

2.3.2.1.4. Recite the following visitor briefing to each person under escort (group briefings are permitted):

2.3.2.1.4.1. I am (state your name), your escort for this visit. Prior to entering the SCIF, I am required to brief you on security procedures and your responsibilities. While you are in the SCIF, you must be under escort by an authorized individual at all times. You must stay with your escort until you depart the area. You must visibly display your 25 AF entry credential on the front of your outermost garment—above the waist—at all times. If you are stopped or challenged by

security forces, you must obey all instructions. Do you have any of the following items with you: personally owned photographic equipment, video equipment, audio recording equipment, computers and associated computer equipment, personal digital assistants, cellular phones, or two-way pagers? These are prohibited items (unless authorized in writing by 25 AF/A2S). You may not carry them into the SCIF. I am now required to search all handcarried items and equipment you plan to take into the SCIF. Be aware, while you are in the SCIF, your person and all your possessions are subject to inspection. Do you have any questions?

2.3.3. Maintain positive control and constant surveillance of escorted personnel at all times while in the SCIF. The number of individuals an escort official can escort at one time is based on the known trustworthiness of the visitors and the ability of the escort to have reasonable control of the visitors, but will not exceed eight (8) visitors.

2.3.3.1. Receive authorization from room occupants prior to permitting escorted personnel entry. Sufficient time will be given to ensure occupants have secured classified material. Announce the presence of escorted personnel to all personnel working in the SCI area being visited. **Note:** Work centers containing escorted personnel will display 25 AFVA 31-101, *Uncleared Visitor Notice,* a flashing or rotating light, or similar device to indicate the continued presence of escorted personnel who are not indoctrinated for SCI material.

2.4. Escorted Exit Procedures. Escort officials will accompany personnel under escort to the same SCIF entry/exit point they initially entered and record “time out” on the AF IMT 1109.

Chapter 3

ESCORT TRAINING/CERTIFICATION

3.1. Escort Training/Certification. Individuals who possess appropriate credentials will be formally trained, tested, and certified annually on the duties and responsibilities of an escort official. 25 AF/A2S develops training and evaluation materials. Security managers administratively track and document training and certification.

Chapter 4

INTRODUCTION/REMOVAL OF ELECTRONIC EQUIPMENT, CONTROLLED ITEMS, AND PROHIBITED ITEMS

4.1. Introduction/Removal of Electronic Equipment.

4.1.1. Driven by the possibility of technical compromise, electronic equipment shall not be routinely carried in or out of the restricted area. Any equipment introduced or removed from the restricted area is subject to physical inspection at any time. To ensure only authorized items are introduced, 25 AF/A2S conducts random and comprehensive inspections of hand-carried items.

4.2. Personally Owned Electronic Equipment and media.

4.2.1. Refer to the 25 AF/A2S SharePoint (**https://lackland.eis.aetc.af.mil/afisr/SO/default.aspx**) for additional information.

4.3. Controlled Items.

4.3.1. Controlled Items may be introduced into the SCIF only after written approval by 25 AF/A2S. **Note 1:** Sample Letters of Authorization are posted on the Non-Secure Internet Protocol Router Network (NIPRNet), Global Data Network Drive, "Security" folder, "Sample Request Letters" folder. Letters of Authorizations can take up to 3 duty days to process. Refer to the 25 AF/A2S SharePoint (**https://lackland.eis.aetc.af.mil/afisr/SO/default.aspx**) for further guidance.

4.4. Prohibited Items.

4.4.1. Refer to the 25 AF/A2S SharePoint (**https://lackland.eis.aetc.af.mil/afisr/SO/default.aspx**) for a list of prohibited items and authorized personal electronic devices (PED).

Chapter 5

INTRUSION DETECTION SYSTEM (IDS)

5.1. Certain areas within the SCIF require personnel to access and secure alarms. Areas protected by alarms are accessed when opening for the day and secured when closing for the day.

5.2. Unit Security Managers will:

5.2.1. Provide training to personnel prior to requesting area/office alarm access for the individual.

5.2.2. Document individual IDS training via local form (see **Attachment 3**); maintain the documentation for program review.

5.2.3. Update 25 AF Form 109, *Security Alarm Emergency Point of Contact (POC)*, and forward to 25 AF/A2S. 25 AF Form 109 will be updated as needed due to changing personnel requirements or not to exceed every 6 months.

5.3. Unit Security Alarm Emergency POCs will (when contacted by 802d Security Forces Squadron (SFS) personnel):

5.3.1. Respond to the affected alarm point within 60 minutes to conduct an internal inspection of the SCIF.

5.3.2. Attempt to determine the probable cause of the alarm activation.

5.3.3. Reset the alarm prior to departure of the response force.

5.4. Personnel accessing alarms will:

5.4.1. Enter the alarmed area and proceed directly to the card reader. LED on the card reader will be “red” if area is alarmed; “green” if the area is accessed. Individuals have 30 seconds from the time they open the door until successful transition of alarms.

5.4.2. Place proximity badge in opposite hand from the one you will use to input your PIN. This prevents multiple readings.

5.4.3. Hold (do not wave) your badge directly in front of the reader until you hear two audible beeps.

5.4.4. Input your 4-digit PIN followed by the pound (#) sign.

5.4.5. Listen for three audible beeps (confirms successful transition from secure to access).

5.4.6. After a slight delay, LED will change from red to green, signaling area has been accessed.

5.5. Personnel securing alarms will:

5.5.1. Ensure there are no personnel left in the area. Conduct an End of Day Security Check IAW **paragraph 7.2**. LED on the card reader will be “green” if the area is accessed. Individuals have 30 seconds from the time the LED changes to “red” to exit the area.

5.5.2. Place proximity badge in opposite hand from the one you will use to input your PIN. This prevents multiple readings.

5.5.3. Hold (do not wave) your badge directly in front of the reader until you hear two audible beeps.

5.5.4. Input your 4-digit PIN followed by the pound (#) sign.

5.5.5. Listen for three audible beeps (confirms successful transition from access to secure).

5.5.6. After a slight delay, LED will change from green to red, signaling area has been secured. Individuals have 30 seconds from the time the LED changes to "red" to exit the area.

Chapter 6

GENERAL POLICY AND PROCEDURES

6.1. Nondiscussion Areas. Nondiscussion areas are clearly defined areas within the SCIF where classified discussions are not authorized due to inadequate sound attenuation. These areas include common areas such as hallways, mechanical rooms, entrance foyers, and emergency exit stairwells. Due to the inability to adequately secure handcarried items, classified information will not be introduced into restrooms or the cafeteria.

6.2. Window Protection. Windows surrounding classified discussion and storage areas will be secured at all times within the SCIF. All windows must be equipped with either blinds and/or curtains. Windows without tinting will have horizontal blinds or curtains closed at all times to prevent outside visual surveillance. Second and 3rd floor windows with tinting may have curtains/blinds open during daylight hours, but closed during hours of darkness or decreased visibility. Horizontal blinds may be angled at 45 degrees as long as visual surveillance is prevented.

6.3. Photography. Photography is prohibited in the 25 AF restricted area/SCIF unless approved by 25 AF Commander (CC) or 25 AF/A2S.

6.3.1. Photography in the SCIF will be unclassified and for official purposes only. Self-help photographic equipment is available for sign out from the 25 AF Public Affairs to authorized personnel with a signed letter on file in the Public Affairs office. Note: 25 AF ECs must be removed prior to still or motion photography.

6.3.2. Photography of classified material or operations for official classified products requires coordination with 25 AF/A2S to preclude unintentional release to unauthorized personnel.

6.4. Freight Elevator Use (building 2000). The exterior doors leading to the outside dock area of the freight elevator are alarmed 24/7. The lock on the exterior doors will be removed at 0700 and returned at 1600 Monday-Friday (excluding holidays and official down days). For access during these hours, contact 802 SFS Alarm Monitor (ext. 977-2307) to request access. Do not handle the steel bar that secures the doors prior to contacting the Alarm Monitor (doing so will generate an alarm).

6.5. Entry/Exit Inspections. Entry/exit inspections serve to deter the introduction of prohibited items/contraband and the removal of classified material. 25 AF/A2S performs random inspections of hand-carried items into and out of the area in conjunction with random antiterrorism measures on normal duty days.

6.6. Lost/Destruction of ECs. Immediately report the loss or destruction of an EC to the unit security manager and the 25 AF SSO.

6.6.1. When an EC is lost, the security manager will direct an inquiry into the loss and will send a copy of the lost badge report (Memorandum for Record), signed by the unit security manager to the badge issuing official (Indoctrination office) within 72 hours. Inquiry and reports must be completed prior to reissuing a new badge.

6.6.2. Personnel with damaged, discolored or excessively worn badges may proceed directly to Visitor Control for reissue.

6.6.3. Within 25 AF-managed and 25 AF-administratively supported SCIFs, personnel who have lost their badges and have yet to be issued a replacement badge may be issued the appropriate Temporary "T" badge corresponding to their respective clearance level.

6.7. Entry Credential Turn-in Procedures. Individuals who no longer need ECs assigned to them (i.e., due to reassignment, separation, or retirement) will report to building 2000, Room 123, Indoctrination/Debrief Office (25 AF/A2S) for debriefing and EC disposition.

Chapter 7

PROTECTION OF CLASSIFIED MATERIAL

7.1. Automated Information System (AIS) Storage Media. Unit personnel who receive computer storage media, such as magnetic or paper-tape reels, cartridges, cassettes, removable hard disks, magnetic cards, diskettes, or removable typewriter cassettes, will ensure the appropriate Standard Form (SF) 700-series classification and SF 711, *Data Descriptor Label,* are attached. Optical Disks (Compact Disc [CD], CD-read-only memory [CD-ROM], and Digital Video Disc [DVD] etc.) will be marked with classification, unit, and duty phone number with a paint pen or permanent marker. Containers holding AIS media will also be marked with appropriate SF 700 series Classification label and SF 711. Handling caveats will be placed on the SF 711.

7.2. Document Destruction. Refer to 25 AFI 16-1401, *Disintegration and Destruction of Classified Material and Media Degaussing,* for proper document destruction procedures.

Chapter 8

COURIERING CLASSIFIED

8.1. 25 AF/A2S Responsibilities :

8.1.1. 25 AF/A2S issues courier authorizations for SCI couriers. If there is a continuing need for couriering SCI information or material, Unit Security Managers must send the request for issuance of the DD Form 2501 to the 25 AF/A2S. This request should be made using memorandum format and sent to 25 AF/A2S identifying the name, grade, social security number (SSN), organization, unit mailing address, and office symbol of the individual. If there is not a continuing need for couriering SCI information or material, a Courier Designation Letter will be issued by the 25 AF/A2S for the individual. Unit Security Managers will request the Courier Designation Letter following the same memorandum format as for the issuance of the DD Form 2501.

8.1.2. 25 AF/A2S grants authorization for couriering of SCI on commercial aircraft on a case-by-case basis.

8.2. User Responsibilities :

8.2.1. When couriering classified information inside buildings 2000 and 2007, use an opaque envelope, marked with appropriate security classification, or required cover sheet.

8.2.2. When transporting SCI outside the SCIF, courier authorization is required. Individuals must contact their Security Manager for the appropriate courier authorization.

Chapter 9

SECURITY BRIEFINGS

9.1. Foreign Travel Briefings. Personnel with SCI access should notify their immediate supervisor and 25 AF/A2S a minimum of 14 days prior to departure. The 25 AF/A2S will give personnel a defensive security briefing before official and unofficial overseas travel. In addition, personnel must review the Department of Defense (DoD) Electronic Foreign Clearance Guide at (**https://www.fcg.pentagon.mil/**) a minimum of 45 days prior to departure to ensure all travel requirements are met.

9.2. Termination Briefings. Upon termination of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment for 45 days or more, unit military personnel and civilian employees will be given a termination briefing, return all classified material, and execute a Security Termination Statement. The 25 AF/A2S will perform the termination briefing.

9.3. Documentation. The security manager documents the training using either a general-purpose form or automated database, listing specific training, name of trainee, name of trainer, and date conducted. Trainees are required to acknowledge training with signature (written or digital) or initials. Records of training will be maintained in the Security Manager's Handbook for one year.

Chapter 10

PERSONNEL PROCESSING

10.1. Badge Issuing Procedures.

10.1.1. Military/Government Civilians Badge Issue.

10.1.1.1. Prior to arrival of inbound personnel, the unit security manager (SM) will submit an indoctrination assist memo with all required information to the Indoctrination Office through the 25 AF A2S/SOPI Workflow NIPRnet email organizational box. The template can be found on Security's SharePoint Page (**https://lackland.eis.aetc.af.mil/afisr/SO/default.aspx**).

10.1.1.2. Upon receipt of the indoctrination assist memo, the Indoctrination Office will verify the individual's SCI eligibility and current Single Scope Background Investigation (SSBI) in Joint Personal Adjudication System (JPAS). If the member's SSBI is out of scope, a periodic reinvestigation (PR) must be submitted and be open in JPAS prior to indoctrination.

10.1.1.3. The Indoctrination office will notify the SM if member requires an indoctrination class or requires just a read-in session during walk-in hours. The member's sponsor will escort the individual to the Indoctrination Office.

10.1.1.4. After indoctrination, JPAS will be updated with SI/TK/G/HCS compartments. The newcomer will be given a 25 AF Form 105 card to take to Visitor Control for issuance of the 25 AF Form 101.

10.1.1.5. Non 25 AF personnel requesting a 25 AF EC will only be issued a picture badge if their "primary place of employment" is located in SCIFs within buildings 2000/2007/2012. For contractors, these SCIFs must be listed as a work location on the DD Form 254. Any request not meeting this requirement will need to be sent to 25 AF/A2S with justification before a picture badge is authorized. Issuance of an EC solely for convenience purposes is not authorized.

10.1.2. Contractor Personnel Badge Issue.

10.1.2.1. The Contracting Officer Representative (COR) receives a list of employees from the contract company which he/she must approve and send an email to the 25 AF/SO-Industrial Security (**AFISRA.so.org@us.af.mil**) for indoctrination.

10.1.2.2. 25 AF/A2S will review the associated DD Form 254, *DoD Contract Security Classification Specification*, and contract documents. In addition, they will verify the SCI eligibility and SSBI currency of each employee in JPAS. If an employee has an out-of-scope investigation a PR must be submitted and open in JPAS prior to indoctrination.

10.1.2.3. At the conclusion of the review, 25 AF/A2S will send the Indoctrination Office a badge request via email.

10.1.2.4. The Indoctrination Office will notify the COR, if the member requires an indoctrination class or a read-in session during walk-in hours. The program

manager/COR will ensure an escort is available to bring the individual to the Indoctrination Office.

10.1.2.5. After indoctrination, JPAS will be updated with SI/TK/G/HCS compartments. The newcomer will be given a 25 AF Form 105 card to take to Visitor Control for issuance of the 25 AF Form 101C. **Note**: Green Picture badges are only issued to SCI-cleared members who possess all SI/TK/G/HCS compartments.

10.2. Unfavorable Administrative Actions. Notify 25 AF/A2S when information is received which places a person's continued eligibility for access to classified information in question. A determination by the Unit Commander, in coordination with the applicable Director, must be made within 20 calendar days whether or not a SIF is justified and whether or not access suspension is warranted.

10.3. Cohabitation/Marriage to Foreign National. Personnel who wish to cohabitate with (living together in a spouse-like relationship) or marry a non-US citizen must obtain authority prior to marriage or cohabitation. Notify 25 AF/A2S using the Letter of Intent format (**Attachment 5**). See 25 AF/A2S SharePoint (**https://lackland.eis.aetc.af.mil/afisr/SO/default.aspx**).

10.4. Continuing Security Responsibilities. Commanders and supervisors must:

10.4.1. Continuously evaluate cleared personnel to ensure that they continue to be trustworthy in accordance with the standards in DOD 5200.2-R, **Chapter 2**.

10.4.2. Notify 25 AF/A2S when information or actions occur that bring into question the person's compliance with prescribed adjudication guidelines.

10.4.3. Ensure unit personnel receive quarterly security training IAW **attachment 4**.

Chapter 11

VISIT PROCEDURES

11.1. Incoming Visits. All visitors to the SCIF/restricted area require verification of eligibility and need to know prior to being granted either unescorted or escorted entry.

11.1.1. Visitors with Top Secret clearances and SCI access transmit visitor information to their local government (military/civilian) point of contact in building 2000/2007/2012. The local POC then forwards that information to the 25 AF/A2S Visit Certifications NIPRNet email for processing.

11.1.1.1. If information is not available in JPAS for the visit, a clearance message should then be sent to 25 AF/A2S for placement on the visitor roster. If the visitor does not want to transmit their visit information via email a visit can be sent via JPAS to SMO code LA0UF21H2, however a local POC must still send the visit information to the 25 AF/A2S Visit Certifications email to validate the need to know. Since visit information is Personally Identifiable Information (PII), it will require the appropriate protection (encryption).

11.1.1.2. Visitor information should include the following: full legal name, status (list rank/grade or contractor, if contractor provide the name of the company), SSN or DoD Common Access Card (CAC) identification number and date of birth, dates of visit, organization being visited and the local government POC information (name, organization and contact number).

11.1.1.3. The 25 AF security office will verify the clearance and will send an email back to the requestor confirming the visit has been approved.

11.1.1.4. Upon arrival, visitors will report to Visitor Control for issue of the 25 AF Form 101T, 101CT, 101DV or 101FT as applicable. These visitors are authorized unescorted entry to areas specified in **paragraph 2.2**. These credentials do not leave the SCIF.

11.1.2. Foreign National visitors with Top Secret clearances and SCI access, Top Secret or Secret collateral clearances will need to coordinate their approvals with their supporting foreign disclosure and release officer (FDRO). The FDRO will then send the embassy certification and visit information to the 25 AF A2S Visit Certifications email. If the visit is for SCI the FDRO will notify the 25 AF/A2S no later than (NLT) 30 days prior to the visit to request that the SCI accesses be submitted.

11.2. Conference Procedures. Personnel hosting SCI/collateral conferences within the SCIF contact 25 AF/A2S for processing of attendee clearances, clearance memorandum and EC issue. ECs issued to conference attendees do not leave the cantonment area.

11.2.1. Conference POCs will:

11.2.1.1. Provide rosters of attendees to include name, rank/grade, and SSN to 25 AF/A2S NLT 3 duty days prior to the start of the event.

11.2.1.2. Hand-carry the verified clearance memorandum to Visitor Control and sign for requisite ECs.

11.2.1.3. Establish procedures to issue, collect, control, and return ECs.

11.3. Outgoing Visits.

11.3.1. 25 AF personnel traveling to locations which require their Top Secret with SCI accesses, Top Secret or Secret collateral clearances be passed to the Temporary Duty (TDY) location need to complete a 25 AF Form 106, *Sensitive Compartmented Information Access Certification*. If the location is requesting a visit be sent in JPAS, the unit security manager will process the request. However, if the location is requesting a message be sent then the 25 AF Form 106 needs to be sent to the 25 AF/A2S Visit Certifications email for processing.

11.3.2. 25 AF personnel traveling to foreign owned SCIFs which require passing of their Top Secret/SCI accesses need to complete a 25 AF Form 106 NLT 30 days prior to the visit and forward to 25 AF/A2S.

Chapter 12

INTELLIGENCE COMMUNITY (IC) BADGE REQUEST

12.1. Intelligence Community (IC) Badge Request. Air Force personnel who make at least 10 visits per month to an IC agency in support of the Air Force IC mission can contact the 25 AF/A2S for information on obtaining an IC badge if required.

Chapter 13

MISCELLANEOUS

13.1. Miscellaneous. The security office has posted a number of sample letters, how to's and training materials on the headquarters domain global data drive in the security folder. Sample letters are also available on the security hill global data drive in the security folder. In addition, the Security Office's SharePoint Page (**https://lackland.eis.aetc.af.mil/afisr/SO/default.aspx**) also provides security guidance and sample letters.

BRADFORD J. SHWEDO, Maj Gen, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDM 5105.21, Volume 1-3, *Sensitive Compartmented Information (SCI) Administrative Security Manual*, 19 October 2012

DoD 5200.01, *DoD Information Security Program*, Volumes 1-4, 19 March 2013

AFPD 16-14, *Security Enterprise Governance*, 24 July 2014

AFPD 31-1, *Integrated Defense*, 28 October 2011

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

AFI 31-101, *Integrated Defense*, 7 March 2013

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 16-1406, *Air Force Industrial Security Program*, 25 August 2015

AFI 33-324, *The Air Force Information Collections and Reports Management Program*, 6 March 2013

AFMAN 33-363, *Management of Records*, 1 March 2008

AFVA 31-107, *Restricted Area Sign*, 15 October 2000

25 AFVA 31-102, *Uncleared Visitor Notice*

25 AFVA31-103, *Entry Credential Background*

25 AFVA 31-104, *Stop-Do Not Use This Machine for Collateral or SCI Classified Reproduction-Stop*

25 AFVA31-105-O, *Know Your Credentials*

25 AFVA 31-106, *Classified Reproduction Rules*

IC Tech Spec-for ICD /ICS 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, 5 May 2011

Prescribed Forms

25 AF Form 101, *Green Unescorted Entry Badge*

25 AF Form 101C, *Green Contractor Picture Badge*

25 AF Form 101CT, *Green Visiting Contractor Badge*

25 AF Form 101DV, *Green Distinguished Visitor Badge*

25 AF Form 101F, *Green Allied Country Picture Badge*

25 AF Form 101FT, *Green Allied Country Visitor Badge*

25 AF Form 101R, *Green Reserve Force Badge*

25 AF Form 101T, *Green Visitor Badge*

25 AF Form 102, *Red Picture Badge*

25 AF Form 102C, *Red Contractor Picture Badge*

25 AF Form 102CT, *Red Visiting Contractor Badge*

25 AF Form 102 DV, *Red Distinguished Visitor Badge*

25 AF Form 102FT, *Red Foreign Visitor Badge*

25 AF Form 102R, *Red Reserve Force Badge*

25 AF Form 102T, *Red Visitor Badge*

25 AF Form 103, *White Picture Badge*

25 AF Form 103DV, *White Distinguished Visitor Badge*

25 AF Form 103E, *White Escort Required Badge*

25 AF Form 104, *Visitor Register Log*

25 AF Form 105, *Entry Authority Entry Credential Issue*

25 AF Form 106, *Sensitive Compartmented Information Access Certification*

25 AF Form 109, *Security Alarm Emergency Point of Contact*

Adopted Forms

DD Form 254, *DoD Contract Security Classification Specification*

DD Form 2501, *Courier Authorization*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

SF 704, *Secret Cover Sheet*

SF 705, *Confidential Cover Sheet*

SF 711, *Data Descriptor Label*

AF Form 144, *Top Secret Access Record and Cover Sheet*

AF Form 847, *Recommendation for Change of Publication*

AF Form 1109, *Visitor Register Log*

AF Form 3535, *Facsimile Electro Mail Transmittal*

Abbreviations and Acronyms

25 AF—Twenty-Fifth Air Force

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AIS—Automated Information System

AT/FP—Antiterrorism Force Protection

ATM—Automated Teller Machine

CAC—Common Access Card

CD—Compact Disc

CD-ROM—Compact Disc, Read-Only Memory

COR—Contracting Officer Representative

DOD—Department of Defense

DVD—Digital Video Disc

EC—Entry Credentials

ECP—Entry Control Point

FDRO—Foreign Disclosure and Release Officer

HQ—Headquarters

IAM—Information Assurance Manager

IAW—In Accordance With

IC—Intelligence Community

ICD—Intelligence Community Directive

IDS—Intrusion Detection System

JBSA—Joint Base San Antonio

JPAS—Joint Personnel Adjudication System

JWICS—Joint Worldwide Intelligence Community System

LED—Light Emitting Diodes

NIPRNet—Non-Secure Internet Protocol Router Network

NLT—No Later Than

OPR—Office of Primary Responsibility

OPSEC—Operation Security

PII—Personal Identifiable Information

PIN—Personal Identification Number

POC—Point of Contact

PR—Periodic Reinvestigation

RDS—Records Disposition Schedule

SAC—Single Agency Check

SAP—Special Access Program

SCI—Sensitive Compartment Information

SCIF—Sensitive Compartmented Information Facility

SF—Standard Form

SFS—Security Forces Squadron

SIF—Security Information File

SM—Security Manager

SOP—Standard Operating Procedure

SSBI—Single Scope Background Investigation

SSN—Social Security Number

SSO—Special Security Office

VC—Visitor Control

Attachment 2

BUILDINGS 2000/2007 ACCESS AND ESCORTING PROCEDURES

Figure A2.1. Buildings 2000/2007 Access and Escorting Procedures.

SCIF DOOR ACCESS: All doors will be secured when not in use with the exception of emergency circumstances. If a door must be left open for any length of time due to emergency or other reasons, then it must be controlled in order to prevent unauthorized personnel from gaining access and unauthorized removal of SCI. Intelligence Community Directive (ICD) 705 states, "Authorized personnel who permit another individual to enter the SCIF shall verify the individual's authorized access." Authorized personnel opening exterior SCIF doors may allow other authorized personnel to enter the SCIF behind them, after validating their entry credentials and photo. Visual recognition is not a sufficient validation – all personnel entering the SCIF must display their EC. "Piggybacking" is authorized for entering and exiting the SCIF with the exception when using the turnstiles for building 2007.

- Whoever opens the SCIF door whether entering or exiting is responsible for ensuring the SCIF door is secured behind or until another authorized user verbally takes charge of the door.

TURNSTILE ENTRY FOR BUILDING 2007 FRONT ENTRANCE: Approach the lane and present your "green picture" EC card and input your 4-digit pin then the # sign. If access is granted, the turnstile arm will retract and you can pass through. If successful the SCIF door will also open allowing access to the building. Ensure the SCIF door secures before walking away. If access is denied, report to Visitor Control (VC) to have your discrepancy resolved. **Note:** Please have another form of ID available either a CAC or valid state driver's licenses.

TURNSTILE EXITING FOR BUILDING 2007 FRONT ENTRANCE: Press the door release bar and push door outward then approach the lane and present your badge to the card reader to exit. If access is granted, the turnstile arm will retract and you can pass through. Ensure the SCIF door secures before walking away.

- Temporary "T" badges will not be removed from the building. All "T" badges must be dropped off inside Visitor Control or dropped off with the issuing satellite account holder. If after duty hours, "T" badges can be dropped off in the door slot of VC.

BUILDING 2000 AND BUILDING 2007 REAR DOOR ENTRY PROCEDURES: Access control is granted through use of proximity access control card readers. Individuals must have a proximity access control badge EC with access privileges granted. PINs are required for use of the EC.

- Place badge in opposite hand from the one inputting your PIN. (Prevents multiple reading)

- Hold your badge directly in front of the reader (Do not wave or flash badge) and you'll hear 2 beeps

- After you hear the two (2) audible beeps, you have five (5) seconds to input your PIN followed by the # sign

- If successful you will hear three (3) audible beeps and the door will automatically open

- If you don't complete the process in five (5) seconds, pause to allow the system to reset, and then re-attempt

Ensure the SCIF door secures before walking away or until another authorized user verbally takes charge of the door.

BUILDING 2000 AND BUILDING 2007 REAR DOOR EXIT PROCEDURES: Press the door release bar and push door outward; exit the SCIF and ensure door secures before walking away or until another authorized user verbally takes charge of the door.

- If someone is waiting to enter as you exit, ensure they have the proper unescorted EC (25 AF Form 101-series green badge) before allowing access

ESCORTING PROCEDURES: ICD 705 further states, "Uncleared personnel shall be escorted at all times by cleared personnel. Additionally, DoDM 5105.21,Vol 2, enclosure 3, paragraph 3b. states, "SCIF access logs must be kept on all visitors."

- "Escort Required" Sign-in Logs will be maintained at 4 locations

-- Location # 1: Inside the foyer at the bottom of the stairs inside the glass doors at building 2000

-- Location # 2: Adjacent to the automated teller machine (ATM) area at building 2000

-- Location # 3: Inside the foyer of building 2007 (courtyard side)

-- Location # 4: Inside the foyer of building 2007 (parking lot side)

- Escorting Procedures for building 2000/2007:

-- All Escorted individuals entering the SCIF via the hallway leading to the cafeteria or via the second/third floors will sign-in at **Location # 1**

-- Non-SCI indoctrinated individuals who enter the non-SCIF area who require escort into any SCIF area (rear area of 2000, 2nd floor entrance above the ATM, etc.) will sign-in at **Location # 2**

-- Individuals who required escort into building 2007 will sign-in at either **Locations # 1, # 3 or # 4**

- Escorted individuals will always be signed-out at the same location they were signed-in

- Phones are located at each location to call for escort officials

- Visitor information must be printed on the sign-in logs to include the "escort official" information

Note: Random checks will be conducted to monitor compliance with escort procedures

I acknowledge I have read the above entry/exit instructions and escort procedures. I also understand my individual responsibilities to ensure access is only granted to authorized individuals.

Printed name: _____

Signature and date: _____

Note: Hand-carry completed forms to Visitor Control at time of badge issue. Once EC is issued, return the form to Unit Security Manager for filing.

Attachment 3

VINDICATOR ALARM ENTRY/EXIT PROCEDURES

Figure A3.1. Vindicator Alarm Entry/Exit Procedures.

ENTRY (ACCESSING)

- Enter alarmed area and proceed directly to the card reader
- LED on the card reader will be "red" if area is alarmed; "green" if area is accessed
- Hold the proximity card directly in front of the card reader
- Listen for two audible beeps (confirms the card has been read)
- Enter four-digit personal PIN followed by the pound sign (#)
- Listen for three audible beeps (confirms successful transition)
- After a slight delay, LED will change from red to green
- Area has been accessed

Note: Individuals have 30 seconds from the time they open the door until successful transition of alarms

EXIT (SECURING)

- Ensure there are no personnel left in the area
- LED on the card reader will be "green" if the area is accessed
- Hold the proximity card directly in front of the card reader
- Listen for two audible beeps (confirms card has been read)
- Enter four-digit personal PIN followed by the pound sign (#)
- Listen for three audible beeps (confirms successful transition)
- After a slight delay, LED will change from green to red
- Area has been secured

Note: Individuals have 30 seconds from the time the LED changes to "red" to exit the area.

I acknowledge I have been properly trained by my Unit Security Manager. I understand the entry/exit procedures and my individual responsibilities as described above.

_____

Signature and date

* Unit Security Managers maintain completed forms.

Attachment 4

ANNUAL SECURITY TRAINING PLAN

A4.1. 1st Quarter.

A4.1.1. Transporting Classified Material.

A4.1.2. Classified Waste.

A4.1.3. Telephone Usage.

A4.1.4. Foreign Contact.

A4.1.5. Alarms and End of Day Security Checks.

A4.1.6. Recognizing SCI.

A4.1.7. Reporting Changes to Your Personal Information.

A4.1.8. Security Violations Introduction.

A4.1.9. Removal of AIS and Media.

A4.2. 2nd Quarter.

A4.2.1. Classified Waste.

A4.2.2. 25 AF Identification Badges.

A4.2.3. Need to Know.

A4.2.4. Prohibited Items.

A4.2.5. Escort Procedures.

A4.2.6. Uncleared Visitors.

A4.2.7. Entry/Exit Inspections.

A4.2.8. Prepublication Review & Resumes.

A4.2.9. AIS/Removable Media Marking.

A4.2.10. Classification Management and Marking Responsibilities.

A4.3. 3rd Quarter.

A4.3.1. Role of the Security Manager.

A4.3.2. Safety/Security Inspections.

A4.3.3. Foreign Intelligence Threats.

A4.3.4. 25 AF and the Public News Media.

A4.3.5. Alarms and End of Day Security Checks.

A4.3.6. Intelligence Oversight.

A4.3.7. Reporting Security Concerns.

A4.3.8. FPCON Definitions & Actions.

A4.3.9. Security Officials.

A4.3.10. Security Forces.

A4.3.11. Reporting Unscheduled Absences.

A4.3.12. Use and Abuse of Drugs.

A4.3.13. Membership in Organizations.

A4.3.14. Off-Limit Establishments.

A4.3.15. Unauthorized Disclosure Training.

A4.4. 4th Quarter.

A4.4.1. Secure FAX Procedures.

A4.4.2. EAP Priority Destruction.

A4.4.3. Annual Clean Out Day.

A4.4.4. Classified Reproduction.

A4.4.5. Password Security.

A4.4.6. Working Papers.

A4.4.7. Local Threat Assessment.

A4.4.8. Derivative Classification Training. **Note:** Training materials are available on the Global Drive Headquarters Domain. You may access this material by opening the "Security" folder, then the "Security Manager" folder.

Attachment 5

LETTER OF INTENT

Figure A5.1. Letter of Intent.

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS 25TH AIR FORCE (ACC)
JOINT BASE SAN ANTONIO – LACKLAND TEXAS

MEMORANDUM FOR 25 AF/A2S

FROM:

SUBJECT: Letter of Intent

1. Request authority to marry (or cohabitation with) to (Mr./Ms. XXXX XXXXX, a non-US person on dd/mm/yy. The following is provided per AFMAN 14-304:

a. Intended spouse:
(1) name:
(2) address
(3) citizenship
(4) vocation

b. Father:
(1) name:
(2) address
(3) citizenship
(4) vocation

c: Mother:
(1) name:
(2) address
(3) citizenship
(4) vocation

d: Brother(s) (list each brother separately)
(1) name:
(2) address
(3) citizenship
(4) vocation

e. Sister(s) (list each sister separately)
(1) name:
(2) address
(3) citizenship
(4) vocation

f. Children (list each separately)
(1) name:
(2) address

(3) citizenship
(4) vocation

2. Does your intended spouse, and his or her immediate family members:

a. Have any political or vocational ties to any government?

b. Advocates for the use of force, or violence, to overthrow the u.s. government?

3. Are your intended spouse, and his or her immediate family members:

a. Subject to physical, mental, or other types of duress by a foreign power?

b. Involved in any criminal activity?

4. What is the nature and extent of contact with immediate family members?

5. Are you currently cohabitating? If so, when was the cohabitant Single Agency Check (SAC) forwarded to OPM?

Signature Block
SSN